UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/202,024 | 08/25/1999 | FRANK SCHAEFER-LORINSER | 2345/45 | 2371 |

26646 7590 05/10/2005

KENYON & KENYON
ONE BROADWAY
NEW YORK, NY 10004

| EXAMINER | |
|---|---|
| BACKER, FIRMIN | |
| ART UNIT | PAPER NUMBER |
| 3621 | |

DATE MAILED: 05/10/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 09/202,024 | SCHAEFER-LORINSER ET AL. | |
| | Examiner | Art Unit | |
| | Firmin Backer | 3621 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *25 April 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *15-29* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *15-29* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. §§ 119 and 120**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

13)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

a) ☐ The translation of the foreign language provisional application has been received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____.
4) ☐ Interview Summary (PTO-413) Paper No(s). _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other:

***Continued Examination Under 37 CFR 1.114***

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after allowance or after an Office action under *Ex Parte Quayle*, 25 USPQ 74, 453 O.G. 213 (Comm'r Pat. 1935). Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, prosecution in this application has been reopened pursuant to 37 CFR 1.114. Applicant's submission filed on April 25th, 2005 has been entered.

***Information Disclosure Statement***

2. The information disclosure statement (IDS) submitted on April 25th, 2005 was filed after the mailing date of the allowance on January 6th, 2005. The submission is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

***Allowable Subject Matter***

3. The indicated allowability of claims 15-29 is withdrawn in view of the newly discovered reference(s) to Davis et al (U.S. Patent No 5,633,930 (*Applicant admitted prior art submitted in Applicant's IDS*). Rejections based on the newly cited reference(s) follow.

***Claim Rejections - 35 USC § 102***

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 15-29 are rejected under 35 U.S.C. 102(e) as being anticipated by Davis et al (U.S. Patent No 5,633,930 (*Applicant admitted prior art submitted in Applicant's IDS*).

6. As per claim 15, Davis et al teach a method for loading (*loading)* input data (*secured data)* into a program (*secure module, 78)* when performing a cash transaction authentication between and electronic cash chip card (*integrated circuit card, fig 1)* and a security module (*security module 78)*, the chip card including a stored credit balance comprising debiting (*debiting)* a requested cash amount from the chip card using a security function (*see fig 1, , column 1 lines 36-44)* adding and storing the requested cash amount (*inserting currency and stored currency into the load value terminal)* in a cash amount summing counter of the security module, subdividing the input data into a plurality of data blocks (*column 4 lines 60-5 line 22)* loading (*loading)* the plurality of data blocks (*keys)* into a linear-feedback shift register (*memory of the integrated circuit, 24)* for performing the program (*column 4 lines 60 5 line 22)* , the linear-feedback shift register having at least one non-linear function cryptographically enhanced using at least one downstream counter introducing at least one additional feedback into the linear-feedback shift register following the at least one downstream counter (*see column 7, 10 line 59-12 line 49)*; and switching off (*power down)* the at least one additional feedback after a predefined first number of pulses of an associated clock (*see column 9 line 58-10 line 9)*.

7. As per claim 16, Davis et al teach a method wherein the input data includes at least a random number, a secret key, and non-secret chip card data (*see column 7, 10 line 59-12 line 49)* (*see column 7, 10 line 59-12 line 49).*

8. As per claim 17, Davis et al teach a method wherein the input data include' s at least a random number, a secret key, and non-secret chip card data, the secret key being associated with the non-secret chip card data, the input data being subdivided so that the non- secret chip card data and the secret key form a first data block and the random number forms a second data block (*see column 7, 10 line 59-12 line 49).*

9. As per claim 18, Davis et al teach a method further comprising calculating an authentication token, wherein a different contents of the at least one downstream counter are used during the loading step than are used after the loading step in the calculating the authentication token (*see column 7, 10 line 59-12 line 49).*

10. As per claim 19, Davis et al teach a method wherein a first downstream counter of the at least one downstream counter counts to 1 (*see column 7, 10 line 59-12 line 49).*

11. As per claim 20, Davis et al teach a method further comprising calculating an authentication token, wherein the at least one downstream counter and the first number of clock pulses are selected so as to enable the calculating of the authentication token to be based on a second number of clock pulses (*see column 7, 10 line 59-12 line 49).*

12. As per claim 21, Davis et al teach a method further comprising outputting bits after the loading is completed (*see column 7, 10 line 59-12 line 49).*

13. As per claim 22, Davis et al teach a method wherein the linear-feedback shift register forms at least part of a circuit, and further comprising outputting bits after the loading of the

blocks is completed; and pulsing the circuit for a third number of pulses of the clock while maintaining the at least one additional feedback between the loading of the blocks and the outputting of the bits (*see column 7, 10 line 59-12 line 49).*

14. As per claim 23, Davis et al teach a method wherein the linear-feedback shift register forms at least part of a circuit, and further comprising: outputting bits after the loading of the blocks is completed; switching off the at least one additional feedback; and pulsing the circuit for a third number of pulses of the clock after the switching off of the at least one additional feedbacks (*see column 7, 10 line 59-12 line 49)*

15. As per claim 24, Davis et al teach a device for loading input data into a program when performing an authentication using a cryptographic MAC function, the device comprising a first counter a linear-feedback shift register having a nonlinear feed-forward function for reading off from the linear-feedback shift register, and for influencing an output of the linear feedback shift register using the first counter, the linear-feedback shift register forming at least part of a circuit, at least one second counter for performing the program, the at least one second counter connected downstream of the linear-feedback shift register; and at least one additional non-linear feedback shift register for cryptographically enhancing the circuit and being connected to the circuit, the at least one additional nonlinear feedback shift register being disconnectable (*see column 7, 10 line 59-12 line 49).*

16. As per claim 25, Davis et al teach a device further comprising a latch, and wherein an additional feedback is tapped off following a first of the at least one second downstream counter and before the latch (*see column 7, 10 line 59-12 line 49).*

17. As per claim 26, Davis et al teach a device further comprising a latch, and wherein an additional feedback is read off from the latch following a first of the at least one second downstream counter (*see column 7, 10 line 59-12 line 49)*.

18. As per claim 27, Davis et al teach a device wherein an additional feedback is read off following a second of the at least one second downstream counter (*see column 7, 10 line 59-12 line 49)*.

19. As per claim 28, Davis et al teach a device further comprising a latch, and wherein an additional feedback is generated as an XOR sum of readouts following a first of the at least one second downstream counter before the latch from the latch following the first of the at least one second downstream counter, and following a second of the at least one second downstream counter (*see column 7, 10 line 59-12 line 49)*.

20. As per claim 29, Davis et al teach a device wherein the first counter and the second counter are subdivided or reduced (*see column 7, 10 line 59-12 line 49)*.

***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Firmin Backer whose telephone number is (571) 272-6703. The examiner can normally be reached on Mon-Thu 9:00 AM - 5:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James Trammell can be reached on (571) 272-6712. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Firmin Backer
Primary Examiner
Art Unit 3621

May 6, 2005